James E. Cecchi
Lindsey H. Taylor
CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
(973) 994-1700

Courtney E. Maccarone
Mark S. Reich
LEVI & KORSINSKY, LLP
55 Broadway, 10th Floor
New York, NY 10006
(212) 363-7500

Attorney for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MEREDITH MURPHY and SCOTT MADLINGER, on behalf of themselves and a class of all others similarly situated, Plaintiffs, v. BETMGM, LLC, Defendant.	Civil Action No. **COMPLAINT and DEMAND FOR JURY TRIAL**

Plaintiffs Meredith Murphy and Scott Madlinger ("Plaintiffs"), individually and on behalf of themselves and all others similarly situated, bring this class action lawsuit against Defendant BetMGM, LLC ("BetMGM" or "Defendant") based upon personal knowledge as to themselves, the investigation of their counsel, and on information and belief as to all other matters.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons who entrusted BetMGM with sensitive personal information which was subsequently exposed in the data breach that was discovered by Defendant on November 28, 2022 (the "Data Breach").

2. Plaintiffs' claims arise from BetMGM's failure to safeguard personally identifying information ("PII") that was entrusted to it in its capacity as a sports betting and igaming operator.

3. The Data Breach was a result of BetMGM's failure to properly secure and safeguard Plaintiffs' and Class Members' sensitive PII stored within its network and servers, including, without limitation, names, postal addresses, email addresses, telephone numbers, dates of birth, hashed Social Security Numbers[1] and account identifiers (such as player ID and screen name).

4. In or around December 21, 2022, Defendant began notifying affected customers that their data had been compromised.

5. In the notice letter, Defendant acknowledged that the breach had taken place in May 2022, and went undiscovered until November 28, 2022.

6. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's network system in a condition vulnerable to cyberattacks.

7. Defendant exposed Plaintiffs and Class Members to harm by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust network systems and security practices in place to safeguard participants' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt notice of the Data Breach.

8. In addition, Plaintiffs' and Class Members' sensitive PII – which was entrusted to Defendant – was compromised and unlawfully accessed due to the Data Breach.

[1] Hashed data is the one-way transformation of data by using a formula to convert the original data into a new and unrecognizable value. However, breaking a hash is possible through various methods. Benjamin Taub, *What Does It Mean To Hash Data And Do I Really Care?*, DATASPACE.COM (Dec. 13, 2017) https://dataspace.com/big-data-applications/what-does-it-mean-to-hash-data/ (last visited Jan. 9, 2023).

9. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of hackers.

10. With personal information available to hackers, bad actors can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class members' names but with another person's photograph, and giving false information to police during an arrest.

11. Consumers who trusted Defendant to securely store their information have suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, out-of-pocket expenses and value of time reasonably incurred to remedy or mitigate the effects of the data breach, loss of value of their personal information, and loss of the benefit of their bargain.

12. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

13. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of others subjected to the Data Breach for negligence, breach of implied contract, and unjust enrichment.

PARTIES

14. Plaintiff Meredith Murphy is a resident of the state of Michigan. Plaintiff Murphy provided her PII to Defendant in or about October of 2022. Plaintiff Murphy received a notice of the Data Breach from BetMGM in December of 2022. Plaintiff Murphy suffered injury and was damaged as a result of Defendant's failure to keep her PII secure.

15. Plaintiff Scott Madlinger is a resident of the state of New Jersey. Plaintiff Madlinger provided his PII to Defendant in approximately 2013. Plaintiff Madlinger received a notice of the Data Breach from BetMGM in December of 2022. Plaintiff Madlinger suffered injury and was damaged as a result of Defendant's failure to keep her PII secure.

16. Defendant BetMGM is a limited liability company registered in the State of New Jersey with a principal place of business in Jersey City, New Jersey.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members; the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs; and at least one Class member is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant because Defendant is headquartered in the state of New Jersey, regularly conducts business in this District, and has extensive contacts with this forum.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

A. The Data Breach

20. Defendant is a sports betting and igaming operator that is a partnership between MGM Resorts International and Entain Holdings and claims it "is revolutionizing sports betting and online gaming in the United States."[2]

21. On or about December 21, 2022, BetMGM sent Plaintiffs and Class Members an email with the subject line "Important Notice About Your Personal Information." The email read, in part:

> We are writing to notify you of an issue that involves certain of your personal information. We have learned that certain BetMGM patron records were obtained in an unauthorized manner. We believe that your information was contained in these records, which may have included details such as name, contact information (such as postal address, email address and telephone number), date of birth, hashed Social Security number, account identifiers (such as player ID and screen name) and information related to your transactions with us. The affected information varied by patron.
>
> We promptly launched an investigation after learning of the matter and have been working with leading security experts to determine the nature and scope of the issue. We learned of the issue on November 28, 2022, and believe the issue occurred in May 2022. We currently have no evidence that patron passwords or account funds were accessed in connection with this issue. Our online operations were not compromised. We are coordinating with law enforcement and taking steps to further enhance our security.

22. In the notice letter, BetMGM acknowledged that it took an unreasonable six months just to discover the Data Breach, never mind notifying impacted customers.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

24. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

---

[2] *Who We Are*, BETMGM, https://www.betmgminc.com/who-we-are/ (last visited January 10, 2023).

25. Plaintiffs and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

B. BetMGM's Electronic Record Security Was Breached

26. Despite BetMGM's promise to employ commercially reasonable methods of safeguarding consumer data, unauthorized parties gained access to consumer data six months before being discovered.[3]

27. In May of 2022, unauthorized parties gained access to BetMGM's consumer data.[4]

28. On November 28, 2022, BetMGM identified the breach of Plaintiffs' and the Class's data, including their PII.[5]

29. In other words, BetMGM did not discover the Data Breach until six months after the start of the Data Breach.

30. On or around December 21, 2022, BetMGM began notifying governments and affected customers of the Data Breach.[6]

31. Plaintiffs received notices of the Data Breach from BetMGM via email on or around December 21, 2022.

C. <u>BetMGM's Response Increased the Potential of Harm</u>

32. As a result of BetMGM's inability to secure Plaintiffs' and Class's PII, Plaintiffs and Class Members incurred unexpected and unnecessary burdens and expenses through trying to secure bank and financial accounts, monitor credit services, verify the security of accounts using

[3] *Privacy Policy*, BETMGM, Aug. 27, 2020, https://www.betmgminc.com/privacy-policy/ (last visited January 10, 2023).
[4] *Notice Regarding Patron Personal Information*, BETMGM (Dec. 21, 2022) https://www.betmgminc.com/notice-regarding-patron-personal-information/ (last visited January 10, 2023).
[5] *Id*.
[6] *Id.*

the PII, and all other activities necessary to mitigate the harm of sensitive information being exposed.

33. Enhancing the danger to Plaintiffs and the Class, BetMGM was incapable of detecting the Data Breach for over six months.

34. From the time BetMGM determined that the Data Breach had taken place, it is unclear how much time BetMGM spent identifying that Plaintiffs' and Class Members' information had been compromised. The only clear detail is that Defendant waited nearly a month after detecting the breach before it began to notify Plaintiffs and the Class.

D. The Harm Caused by the Data Breach, Now and Going Forward

35. Victims of data breaches are susceptible to becoming victims of identity theft.

36. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[7]

37. The type of data that was accessed and compromised here – such as, full name, contact information, date of birth, and hashed Social Security number – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

[7] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited January 10, 2023).

38. Plaintiffs and Class members face a substantial risk of identity theft given that their hashed Social Security numbers,[8] addresses, and dates of birth were compromised. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

39. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

40. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors sell that information for profit.[9]

41. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[10]

---

[8] Breaking a hash is "absolutely" possible, as discussed in: Benjamin Taub, *What Does It Mean To Hash Data And Do I Really Care?*, DATASPACE.COM (Dec. 13, 2017) https://dataspace.com/big-data-applications/what-does-it-mean-to-hash-data/ (last visited Jan. 9, 2023).

[9] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited January 5, 2023).

[10] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018) https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited January 10, 2023).

42. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

43. A compromised or stolen Social Security number cannot be addressed as simply as, perhaps, a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

44. The PII compromised in the Data Breach demands a high price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[14]

---

[11] *Id.*

[12] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited January 10, 2023).

[13] *Id.*

[14] *Experts advise compliance not same as security*, RELIAS MEDIA https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (Last visited January 10, 2023).

45. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[15]

46. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[16] Defendant did not rapidly report to Plaintiffs and Class members that their PII had been stolen. Instead, BetMGM delayed notification of the Data Breach.

47. As a result of the Data Breach, the PII of Plaintiffs and Class members have been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. improper disclosure of their PII;

e. loss of privacy;

f. trespass and damage their personal property, including PII;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft

[15] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (Last visited January 10, 2023).
[16] *Id.*

protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market; and

i. damages to and diminution in value of their PII entrusted to Defendant.

48. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

49. Defendant disregarded the rights of Plaintiffs and Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

50. The actual and adverse effects to Plaintiffs and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiffs and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit

reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

51. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

52. All persons in the United States whose PII was compromised as a result of the Data Breach (the "Class").

53. Specifically excluded from the Class are BetMGM, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers or entities controlled by BetMGM, and their heirs, successors, assigns, or other persons or entities related to or affiliated with BetMGM and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

54. Plaintiffs reserve the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

55. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

56. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts

are presently within the sole knowledge of Defendant, Plaintiffs estimate that the Class is comprised of thousands of Class members. The Class is sufficiently numerous to warrant certification.

57. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of other Class Members because they all had their PII compromised as a result of the Data Breach. Plaintiffs are members of the Class and their claims are typical of the claims of the members of the Class. The harm suffered by Plaintiffs is similar to that suffered by all other Class members that was caused by the same misconduct by Defendant.

58. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs has no interests antagonistic to, nor in conflict with, the Class. Plaintiffs has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

59. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

60. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether BetMGM failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether BetMGM's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether BetMGM's storage of Class Member's PII was done in a negligent manner;

d. Whether BetMGM had a duty to protect and safeguard Plaintiffs' and Class Members' PII?

e. Whether BetMGM's conduct was negligent;

f. Whether BetMGM breached its implied contract with Plaintiffs and Class Members?

g. Whether BetMGM took sufficient steps to secure its customers' PII;

h. Whether BetMGM was unjustly enriched; and

i. The nature of relief, including damages and equitable relief, to which Plaintiffs and members of the Class are entitled.

61. Information concerning BetMGM's policies is available from BetMGM's records.

62. Plaintiffs knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

63. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for BetMGM. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

64. BetMGM has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

65. Given that BetMGM has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

COUNT I
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and All Class Members)

66. Plaintiffs hereby incorporate all other paragraphs of this Complaint and restate them as if fully set forth herein.

67. In connection with receiving online betting and/or igaming services from BetMGM, Plaintiffs and all other Class members entered into implied contracts with Defendant.

68. Pursuant to these implied contracts, Plaintiffs and Class members provided BetMGM with their PII in order use its services, for which BetMGM is compensated. In exchange, BetMGM agreed to, among other things, and Plaintiffs understood that BetMGM would: (1) provide services to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

69. In the ordinary course of providing its services, customers provide Defendant with their PII.

70. Implied in these exchanges was a promise by Defendant to take reasonable steps to ensure that the PII of Plaintiffs and Class members in its possession was secure.

71. Implied in these exchanges was a promise by Defendant to ensure the PII of Plaintiffs and Class members in its possession was only used to provide the agreed-upon services, and that Defendant would take adequate measures to protect Plaintiffs' and Class members' PII.

72. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiffs' and Class members' PII to be accessed in the Data Breach.

73. Indeed, implicit in the agreement between Defendant and its customers was the obligation that both parties would maintain information confidentially and securely.

74. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiffs and Class members would provide their PII in exchange for services by Defendant. These agreements were made by Plaintiffs and Class members as customers of Defendant's.

75. It is clear by these exchanges that the parties intended to enter into an agreement and mutual assent occurred. Plaintiffs and Class members would not have disclosed their PII to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class members' PII if it did not intend to provide Plaintiffs and Class members with its services.

76. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure and/or use.

77. Plaintiffs and Class members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

78. Plaintiffs and Class members would not have entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII.

79. Defendant breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII.

80. Defendant's failure to implement adequate measures to protect the PII of Plaintiffs and Class members violated the purpose of the agreement between the parties.

81. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class members' PII, which Plaintiffs and Class members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiffs and Class members.

82. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiffs and Class members, Plaintiffs and the Class members suffered damages as described in detail above.

COUNT II
NEGLIGENCE
(On behalf of Plaintiffs and All Class Members)

83. Plaintiffs hereby incorporate all other paragraphs of this Complaint and restate them as if fully set forth herein.

84. Plaintiffs bring this count individually and on behalf of the Class Members.

85. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

86. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII.

87. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' PII within its possession was compromised and precisely the type(s) of information that were compromised.

88. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its customers' PII.

89. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

90. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

91. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII.

92. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards;

d. Failure to implement adequate response procedures after discovery of a data breach, including providing timely notice to Class Members.

93. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII within Defendant's possession.

94. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' PII.

95. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

96. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs and Class Members' PII would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

97. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII would result in injuries to Plaintiffs and Class Members.

98. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII to be compromised.

99. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

100. As a result of Defendant's failure to timely notify Plaintiffs and Class Members that their PII had been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

101. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiffs and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; and future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiffs and All Class Members)

102. Plaintiffs hereby incorporate all other paragraphs of this Complaint and restate them as if fully set forth herein.

103. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

104. Plaintiffs conferred a benefit upon Defendant by using Defendant's services.

105. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs.

106. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of money it received as a result of Plaintiffs and Class Members using its service because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII or used Defendant's services had they known Defendant would not adequately protect their PII.

107. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: January 23, 2023

CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.

By: /s/ *James E. Cecchi*
James E. Cecchi
Lindsey H. Taylor
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
Email: jcecchi@carellabyrne.com
Email: ltaylor@carellabyrne.com

Courtney E. Maccarone
Mark S. Reich*
LEVI & KORSINSKY, LLP
55 Broadway, 10th Floor
New York, NY 10006
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com
Email: mreich@zlk.com

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice* application forthcoming.